IN THE CLAIMS

1. (previously presented) An information processing apparatus for carrying out secure transmission of content to another apparatus over a network, said information processing apparatus comprising:

an encryption unit operable to encrypt the content;

an authentication unit operable to receive authentication information from the another apparatus when the another apparatus requests permission to receive the encrypted content, and to determine whether the authentication information is valid;

a first obtaining unit operable to obtain identification information of the another apparatus from the authentication information when the authentication information is valid and to determine whether the identification information of the another apparatus is already stored in a storage unit;

a transmitting unit operable to transmit a decryption key to the another apparatus when the authentication information is valid, the decryption key being needed to decrypt the encrypted content; and

a first counting unit operable to increment a count of a total number of apparatuses to receive the encrypted content by one when the identification information of the another apparatus is not already stored in said storage unit and the count of the total number of apparatuses is less than a maximum value;

said storage unit being operable to store the identification information of the another apparatus when the identification information of the another apparatus is not already stored in said storage unit.

2. (previously presented) An information processing apparatus according to Claim 1, wherein the another apparatus is operable to transmit the encrypted content to a plurality of

further apparatuses over the network, and said information processing apparatus further comprises:

a second obtaining unit operable to obtain a first value and a second value from the another apparatus when the authentication information is valid, the first value being a number of apparatuses in the plurality of further apparatuses that are newly requesting to receive the encrypted content, and the second value being a total number of apparatuses in the plurality of further apparatuses;

a second counting unit operable to increment the count of the total number of apparatuses to receive the encrypted content by the first value when (i) the sum of the first value and the count of the total number of apparatuses is at most equal to the maximum value and (ii) the identification information of the another apparatus is already stored in said storage unit,

said second counting unit being operable to increment the count of the total number of apparatuses to receive the encrypted content by the second value when (i) the sum of the second value and the count of the total number of apparatuses is at most equal to the maximum value and (ii) the identification information of the another apparatus is not already stored in said storage unit.

3. (previously presented) An information processing apparatus according to Claim 1, further comprising:

an information updating unit operable to delete the identification information stored in said storage unit and to reset the count of the total number of apparatuses to receive the encrypted content when said decryption key is changed.

4. (previously presented) A method for carrying out secure transmission of content from an information processing apparatus to another apparatus over a network, said method comprising:

encrypting the content;

receiving authentication information from the another apparatus when the another apparatus requests permission to receive the encrypted content;

determining whether the authentication information is valid;

obtaining identification information of the another apparatus from the authentication information when the authentication information is valid;

determining whether the identification information of the another apparatus is already stored;

transmitting a decryption key to the another apparatus when the authentication information is valid, the decryption key being needed to decrypt the encrypted content;

incrementing a count of a total number of apparatuses to receive the encrypted content by one when the identification information of the another apparatus is not already stored and the count of the total number of apparatuses is less than a maximum value; and

storing the identification information of the another apparatus when the identification information of the another apparatus is not already stored.

5. (previously presented) A recording medium having recorded thereon a program for executing a method for carrying out secure transmission of content from an information processing apparatus to another apparatus over a network, said method comprising:

encrypting the content;

receiving authentication information from the another apparatus when the another apparatus requests permission to receive the encrypted content;determining whether the authentication information is valid;

obtaining identification information of the another apparatus from the authentication information when the authentication information is valid;

determining whether the identification information of the another apparatus is already stored;

transmitting a decryption key to the another apparatus when the authentication information is valid, the decryption key being needed to decrypt the encrypted content;

incrementing a count of a total number of apparatuses to receive the encrypted content by one when the identification information of the another apparatus is not already stored and the count of the total number of apparatuses is less than a maximum value; and

storing the identification information of the another apparatus when the identification information of the another apparatus is not already stored.

6. (currently amended) An information processing apparatus for carrying out secure receiving of content from a first apparatus over a first network and for carrying out secure transmission of the content to a second apparatus over a second network, said information processing apparatus comprising:

a first transmitting unit operable to transmit to the first apparatus a request for permission to receive the content;

a first authentication unit operable to perform a first authentication procedure with the first apparatus;

a receiver operable to receive a first decryption key from the first apparatus when the first authentication procedure is successful;

a decryption unit operable to use the first decryption key to decrypt encrypted content received from the first apparatus;

~~an~~ reencryption unit operable to reencrypt the decrypted content;

a second authentication unit operable to receive authentication information from the second apparatus when a request for permission to receive the content is made from the second apparatus and to determine whether the authentication information is valid;

a first obtaining unit operable to obtain identification information of the second apparatus from the authentication information when the authentication information is valid and to determine whether the identification information of the second apparatus is already stored in a storage unit;

a second transmitting unit operable to transmit a second decryption key to the second apparatus when the authentication information is valid, the second decryption key being needed to decrypt the reencrypted content; and

a first counting unit operable to increment a count of a number of apparatuses to receive the reencrypted content by one when the identification information of the second apparatus is not already stored in said storage unit and the count of the total number of apparatuses is less than a maximum value;

said storage unit being operable to store the identification information of said second apparatus when the identification information of the second apparatus is not already stored in said storage unit.

7. (cancelled)

8. (previously presented) An information processing apparatus according to Claim 6, further comprising:

a third transmitting unit operable to transmit, to the first apparatus, the count of the number of apparatuses to receive the content.

9. (previously presented) An information processing apparatus according to Claim 6, further comprising:

an information updating unit operable to delete the identification information stored in said storage unit and to

reset the count of the number of apparatuses to receive the reencrypted content when said second decryption key is changed.

10. (previously presented) A method for carrying out secure receiving of content from a first apparatus over a first network and for carrying out secure transmission of the content to a second apparatus over a second network, said method comprising:

transmitting to the first apparatus a request for permission to receive the content;

performing a first authentication procedure with the first apparatus;

receiving a first decryption key from the first apparatus when the first authentication procedure is successful;

decrypting, using the first decryption key, encrypted content received from the first apparatus;

reencrypting the decrypted content;

receiving authentication information from the second apparatus when a request for permission to receive the content is made from the second apparatus;

determining whether the authentication information is valid;

obtaining identification information of the second apparatus from the authentication information when the authentication information is valid ;

determining whether the identification information of the second apparatus is already stored;

transmitting a second decryption key to the second apparatus when the authentication information is valid, the second decryption key being needed to decrypt the reencrypted content;

incrementing a count of a number of apparatuses to receive the reencrypted content by one when the identification information of the second apparatus is not already stored in

said storage unit and the count of the total number of apparatuses is less than a maximum value;

storing the identification information of the second apparatus when the identification information of the second apparatus is not already stored.

11. (previously presented) A recording medium having recorded thereon a program for executing a method for carrying out secure receiving of content from a first apparatus over a first network and for carrying out secure transmission of the content to a second apparatus over a second network, said method comprising:

transmitting to the first apparatus a request for permission to receive the content;

performing a first authentication procedure with the first apparatus;

receiving a first decryption key from the first apparatus when the first authentication procedure is successful;

decrypting, using the first decryption key, encrypted content received from the first apparatus;

reencrypting the decrypted content;

receiving authentication information from the second apparatus when a request for permission to receive the content is made from the second apparatus;

determining whether the authentication information is valid;

obtaining identification information of the second apparatus from the authentication information when the authentication information is valid ;

determining whether the identification information of the second apparatus is already stored;

transmitting a second decryption key to the second apparatus when the authentication information is valid, the

second decryption key being needed to decrypt the reencrypted content;

incrementing a count of a number of apparatuses to receive the reencrypted content by one when the identification information of the second apparatus is not already stored in said storage unit and the count of the total number of apparatuses is less than a maximum value;

storing the identification information of the second apparatus when the identification information of the second apparatus is not already stored.

12. (previously presented) An information processing apparatus according to Claim 1, wherein the authentication information includes first authentication information and second authentication information, and said authentication unit includes:

a first authentication subunit operable to receive the first authentication information from the another apparatus when the another apparatus requests permission to receive the encrypted content, and to determine whether the first authentication information is valid; and

a second authentication subunit operable to transmit a request for the second authentication information to the another apparatus when the first authentication information is valid, to receive the second authentication information from the another apparatus, and to determine whether the second authentication information is valid;

said transmitting unit being operable to transmit the decryption key to the another apparatus when the second authentication information is valid.

13. (previously presented) An information processing apparatus according to Claim 6, wherein the authentication information includes first authentication information and second

authentication information, and said second authentication unit includes:

a first authentication subunit operable to receive the first authentication information from the second apparatus when the second apparatus requests permission to receive the content, and to determine whether the first authentication information is valid; and

a second authentication subunit operable to transmit a request for the second authentication information to the second apparatus when the first authentication information is valid, to receive the second authentication information from the second apparatus, and to determine whether the second authentication information is valid;

said second transmitting unit being operable to transmit the second decryption key to the second apparatus when the second authentication information is valid.